PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-212458
(43)Date of publication of application : 15.08.1997

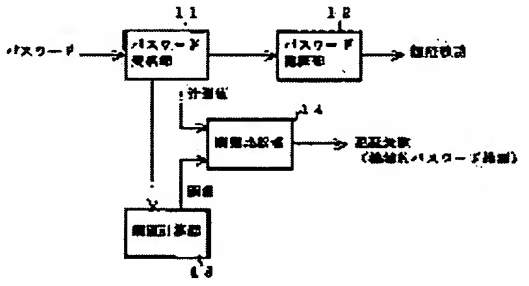
(51)Int.Cl. G06F 15/00
G06F 1/00
G06F 12/14

(21)Application number : 08-014516
(22)Date of filing : 30.01.1996

(71)Applicant : TOSHIBA CORP
(72)Inventor : SATO TATSUO

(54) PASSWORD AUTHENTICATING METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an authenticating method which can prevent system resources from illegally being used by mechanical password anticipation without giving disadvantages to a legal user.
SOLUTION: A password reception part 11 always counts the frequency (a) of password reception per unit time and a threshold value comparison part 14 compares the counted password reception frequency (a) per unit time with a threshold value G. The threshold value G is set suitably on the assumption that the password reception frequency per unit time at the time of mechanical password anticipation by a program, etc., is larger than the password reception frequency per unit time at the time of manual input. When a >G, it is considered that the mechanical password anticipation is performed and respective inputted passwords are invalidated. Consequently, the execution of the mechanical password anticipation is stopped.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平9－212458

(43)公開日　平成９年(1997)８月15日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ	15/00	３３０		Ｇ０６Ｆ	15/00	３３０Ｂ
	1/00	３７０			1/00	３７０Ｅ
	12/14	３２０			12/14	３２０Ｃ

審査請求　未請求　請求項の数７　ＯＬ　（全 13 頁）

(21)出願番号　特願平8－14516

(22)出願日　平成８年(1996)１月30日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　佐藤　龍雄
東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内

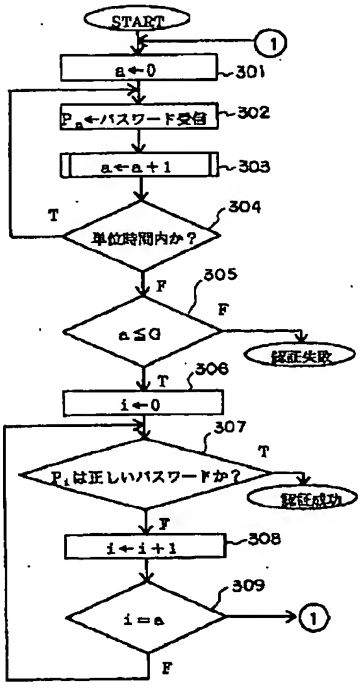
(74)代理人　弁理士　須山　佐一

(54)【発明の名称】　パスワード認証方法

(57)【要約】

【課題】　従来のパスワード認証方法はプログラム等による機械的パスワード推測に脆い点が課題とされていた。

【解決手段】　パスワード受信部１１にて随時、単位時間当たりのパスワード受信回数ａを計数し、計数した単位時間当たりのパスワード受信回数ａと閾値Ｇとを閾値比較部１４にて比較する。閾値Ｇはプログラム等による機械的パスワード推測時の単位時間当たりのパスワード受信回数が手入力時の単位時間当たりのパスワード受信回数より多いという仮定に基づいて最適に設定される。比較の結果ａ＞Ｇの場合は機械的パスワード推測が行われているとみなし、入力された各パスワードを無効化する。これにより機械的パスワード推測の実行が阻止される。



1

【特許請求の範囲】
【請求項１】　入力パスワードと登録パスワードとを照合して前記入力パスワードに対する認証結果を得るパスワード認証方法において、
単位時間当たりに入力されたパスワードの数を計数し、計数した入力パスワード数と予め設定された閾値とを比較し、前記入力パスワード数が前記閾値より大きい場合、前記単位時間分の入力パスワードを無効化することを特徴とするパスワード認証方法。
【請求項２】　入力パスワードと登録パスワードとを照合して前記入力パスワードに対する認証結果を得るパスワード認証方法において、
入力された各パスワードの入力時間間隔を測定し、測定したパスワード入力時間間隔の値と予め設定された閾値とを比較し、前記パスワード入力時間間隔の値が前記閾値より小さい場合、前記入力された各パスワードを無効化することを特徴とするパスワード認証方法。
【請求項３】　入力パスワードと登録パスワードとを照合して前記入力パスワードに対する認証結果を得るパスワード認証方法において、
入力された各パスワードの入力時間間隔のばらつきの大きさを測定し、測定したパスワード入力時間間隔のばらつきの大きさと予め設定された閾値とを比較し、前記パスワード入力時間間隔のばらつきの大きさが前記閾値より小さい場合、前記入力された各パスワードを無効化することを特徴とするパスワード認証方法。
【請求項４】　入力パスワードと登録パスワードとを照合して前記入力パスワードに対する認証結果を得るパスワード認証方法において、
入力された各パスワード間の類似度を求め、求めた類似度の値と予め設定された閾値とを比較し、その比較結果に基づいて前記入力された各パスワードを無効化するか否かを判定することを特徴とするパスワード認証方法。
【請求項５】　請求項４記載のパスワード認証方法において、
前記各パスワード間の類似度の値は、前記各パスワード間の共通する位置の文字が一致しているものの数から求められ、求めた類似度の値が前記閾値より大きい場合に前記入力された各パスワードを無効化することを特徴とするパスワード認証方法。
【請求項６】　請求項４記載のパスワード認証方法において、
前記各パスワード間の類似度の値は、入力されたｎ（但し、ｎ≧２）個のパスワードのうちそのパスワード単語が連続して辞書編纂順となっているものの数から求められ、求めた類似度の値が前記閾値より大きい場合、前記入力されたｎ個のパスワードを無効化することを特徴とするパスワード認証方法。
【請求項７】　請求項４記載のパスワード認証方法において、

2

前記各パスワード間の類似度の値は、入力されたｎ（但し、ｎ≧２）個のパスワード間において文字列が完全に一致する２つのパスワードの組み合わせの数から求められ、求めた類似度の値が前記閾値より小さい場合、前記入力されたｎ個のパスワードを無効化することを特徴とするパスワード認証方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、コンピュータシステムの技術分野に属するパスワード認証方法に関する。
【０００２】
【従来の技術】アクセス権限を必要とするコンピュータシステムにおいては、アクセス権限を持つ利用者を識別するためにパスワードと呼ばれる有限長の文字列を用いた利用者の認証確認を行っている。このパスワードを用いた認証方法において、利用者より入力されたパスワードは予め登録されているパスワードと照合され、両パスワードが一致した場合、当該利用者に対してアクセス権限が与えられる。
【０００３】しかし、パスワードは第三者によって推測される危険がある。例えば、全ての文字の組み合わせを生成して順に入力して行けば、最終的には正しいパスワードが突き止められてしまう確率が高い。また、パスワードとして単語が使用されることが多い点もパスワード推測を容易にする要因の一つとなっている。
【０００４】これらのパスワード推測の予防策としては、パスワードの文字数を多くする方法、辞書上の単語以外の文字列を使用する方法等が最も単純な方法として考えられる。しかし、これらの方法は正規の利用者にとってパスワードの使い勝手が悪くなり、利用者に受け入れられない場合が多い。また、プログラム等の機械的パスワード推測の下では無力に等しいとも言える。
【０００５】そこで、この機械的パスワード推測の防止策として、連続して一定回数間違ったパスワードが入力された場合に以降のパスワード入力を受け付けないようする方法が提案されている。ところが、この方法においては、正規の利用者の不注意によるパスワード誤入力によってもパスワード入力が不可となってしまい、トラブルの原因となる。
【０００６】
【発明が課題しようとする課題】以上のように、従来のパスワード認証方法は特に機械的パスワード推測に脆く、その対策が強い要望として発生している。
【０００７】本発明はこのような課題を解決するためのもので、正規の利用者にデメリットを与えることなく機械的パスワード推測によるシステム資源の不正利用を防止することのできるパスワード認証方法の提供を目的とする。
【０００８】
【課題を解決するための手段】上記目的を達成するため

に、本発明のパスワード認証方法は、単位時間当たりに入力されたパスワードの数を計数し、計数した入力パスワード数と予め設定された閾値とを比較し、入力パスワード数が閾値より大きい場合、前記単位時間分の入力パスワードを無効化する点を特徴とする。

【０００９】この発明は、プログラム等による機械的パスワード推測時の単位時間当たりのパスワード受信回数が手入力時の単位時間当たりのパスワード受信回数より多い点に鑑みて構成され、単位時間当たりのパスワード受信回数が予め設定された閾値よりも大きい場合に入力パスワードを無効化して、機械的パスワード推測の実行を阻止する。

【００１０】また、本発明のパスワード認証方法は、入力された各パスワードの入力時間間隔を測定し、測定したパスワード入力時間間隔の値と予め設定された閾値とを比較し、パスワード入力時間間隔の値が閾値より小さい場合、入力された各パスワードを無効化することを特徴とする。

【００１１】この発明は、プログラム等による機械的パスワード推測時のパスワード入力時間間隔が手入力時のパスワード入力時間間隔より短い点に鑑みて、パスワード入力時間間隔の値が閾値より小さい場合に入力された各パスワードを無効化して、機械的パスワード推測の実行を阻止する。

【００１２】さらに、本発明の本発明のパスワード認証方法は、入力された各パスワードの入力時間間隔のばらつきの大きさを測定し、測定したパスワード入力時間間隔のばらつきの大きさと予め設定された閾値とを比較し、パスワード入力時間間隔のばらつきの大きさが閾値より小さい場合、入力された各パスワードを無効化する点に特徴がある。

【００１３】この発明は、プログラム等による機械的パスワード推測時のパスワード入力時間間隔のばらつきが手入力時のパスワード入力時間間隔のばらつきより短い点に鑑みて、パスワード入力時間間隔のばらつきの大きさが閾値より小さい場合、入力された各パスワードを無効化して、機械的パスワード推測の実行を阻止する。さらに、本発明のパスワード認証方法は、入力された各パスワード間の類似度を求め、求めた類似度の値と予め設定された閾値とを比較し、その比較結果に基づいて入力された各パスワードを無効化するか否かを判定する点を特徴とする。ここで、各パスワード間の類似度の値は、各パスワード間の共通する位置の文字が一致しているものの数から求めることができる。機械的パスワード推測は例えば１文字ずつパスワードを変えながら行われることが多い。したがって、求めた類似度の値が閾値より大きい場合、入力された各パスワードを無効化することで、機械的パスワード推測の実行を阻止することができる。

【００１４】また、各パスワード間の類似度の値は、入力されたｎ（但し、ｎ≧２）個のパスワードのうちそのパスワード単語が連続して辞書編纂順となっているものの数からも求めることができる。この場合も同様に、求めた類似度の値が前記閾値より大きい場合、入力されたｎ個のパスワードを無効化する。機械的パスワード推測においては辞書の単語を編纂順に入力することが考えられ、このような機械的パスワード推測を本発明のパスワード認証方法は極めて高精度に検出することが可能である。

【００１５】さらに、各パスワード間の類似度の値は、入力されたｎ（但し、ｎ≧２）個のパスワード間において文字列が完全に一致する２つのパスワードの組み合わせの数から求めることができる。この発明は、機械的パスワード推測では同じパスワードが入力されることは無いという仮説に基づくものであり、この場合、求めた類似度の値が前記閾値より小さい場合に入力されたｎ個のパスワードを無効化するものとする。

【００１６】

【発明の実施の形態】以下、本発明の実施の形態について説明する。

【００１７】図１は本実施形態のパスワード認証方法を採用したコンピュータシステムの構成を示している。同図において、１は利用者側のクライアント計算機、２はクライアント計算機１の利用者より入力されたパスワードの認証手続きを行うサーバ計算機である。サーバ計算機２はパスワードの認証結果をクライアント計算機１に返すと共に、パスワード認証に成功つまり入力パスワードが登録パスワードと一致した場合にサーバ計算機２が管理しているデータベース３等のシステム資源へのアクセス権限をクライアント計算機１上の利用者に与える。

【００１８】図２はサーバ計算機２内のパスワード認証機構の構成を示したブロック図である。１１はクライアント計算機１より送信されたパスワードを受信するパスワード受信部、１２は受信パスワードと登録パスワードとを照合して両者が一致した場合にパスワード認証成功を出力するパスワード認証部、１３は機械的パスワード推測の判定用の閾値を設定する閾値計算部、１４はパスワード受信部１１にて求められた受信パスワードに関する情報（単位時間当たりのパスワード受信回数、各パスワードの入力時間間隔、パスワード間の類似度）の測定値と前記閾値との比較を通じて機械的パスワード推測を検出する閾値比較部である。

【００１９】次に、受信パスワードに関する情報として“単位時間当たりのパスワード受信回数”を用いた場合のパスワード認証方法の実施形態１について説明する。

【００２０】（実施形態１－１）図３は実施形態１－１のパスワード認証方法の手順を示すフローチャートである。パスワード受信部１１は、随時、単位時間当たりのパスワード受信回数ａを計数している（ステップ３０１～３０４）。閾値比較部１４は、パスワード受信部１１

より計数された単位時間当たりのパスワード受信回数ａと閾値計算部１３にて予め設定された閾値Ｇとを比較する（ステップ３０５）。ここで閾値Ｇは、プログラム等による機械的パスワード推測時の単位時間当たりのパスワード受信回数が手入力時の単位時間当たりのパスワード受信回数より多いという仮定に基づいて最適に設定される。その設定方法については後で詳しく述べる。

【００２１】上記比較の結果、ａ＞Ｇの場合は、機械的パスワード推測が行われているとみなし、認証失敗を判定する。また、ａ≦Ｇの場合は、受信したパスワードをパスワード認証部１２に送る。パスワード認証部１２は受信パスワードの中に正しいパスワードがあれば認証成功と判断し、システム資源のアクセス権限をクライアント計算機１の利用者に与える。また、受信パスワードの中に正しいパスワードがなければ再びパスワード受信を行う（ステップ３０６～３０９）。

【００２２】このようにパスワード認証を行う前に、単位時間当たりのパスワード受信回数ａと閾値Ｇとを比較して機械的パスワード推測が行われていることを判断することで、機械的パスワード推測によって偶然正しいパスワードが入力されても、この場合は認証失敗と判断され、システム資源のアクセス権限を不正な利用者に与えることを防止できる。

【００２３】（実施形態１－２）次に、受信パスワードに関する情報として“単位時間当たりのパスワード受信回数”を用いた場合のもう一つのパスワード認証方法について説明する。

【００２４】図４はこのパスワード認証方法の手順を示すフローチャートである。パスワード受信部１１は、単位時間当たりのパスワード受信回数ａを計数すると共に、パスワードを１つ受信する度にその受信パスワードをパスワード認証部１２に送ってパスワード認証を実施させる。受信パスワードが正しいパスワードがあれば認証成功を判断し、システム資源のアクセス権限をクライアント計算機１の利用者に与える。また、受信パスワードが誤ったパスワードであれば再びパスワード受信を行う（ステップ４０１～４０５）。パスワード受信部１１は、単位時間内に正しいパスワードが入力されなかった場合に、計数した単位時間当たりのパスワード受信回数ａを閾値比較部１４に送る。閾値比較部１４は、パスワード受信部１１より受けとった単位時間当たりのパスワード受信回数ａと閾値計算部１３にて予め設定された閾値Ｇとを比較し（ステップ４０６）、ａ＞Ｇの場合、機械的パスワード推測が行われているとみなし、認証失敗を判定する。

【００２５】このパスワード認証方法によれば、最初の単位時間を除けば、機械的パスワード推測によって偶然正しいパスワードが入力されても認証失敗を判定することができる。なお、最初の単位時間に機械的パスワード推測によって偶然正しいパスワードが入力される確率は極めて低く実用上全く問題はない。また、このパスワード認証方法は、前記の方法と比較した場合、単位時間分の遅延を有することなくパスワードの認証結果を利用者に提供することができ、利用者に違和感を与えない方法と言える。

【００２６】次に、閾値の設定方法について述べる。この閾値は、プログラム等による機械的パスワード推測時の単位時間当たりのパスワード受信回数が手入力時の単位時間当たりのパスワード受信回数より多いという仮定に基づいて設定される。その具体的な算出方法を以下に挙げる。

【００２７】①単位時間当たりの人間によるパスワード入力回数の平均値と標準偏差から、平均値＋標準偏差×ｎ（ｎは任意の数値）を求め、これを閾値とする。

【００２８】②単位時間当たりの機械的パスワード推測によるパスワード入力回数の平均値と標準偏差から、平均値＋標準偏差×ｎ（ｎは任意の数値）を求め、これを閾値とする。

【００２９】③方法①と方法②で求めた各閾値の間の任意の値を閾値とする。この場合、①におけるｎの値は②におけるｎの値は同じでなくてもよい。

【００３０】これらの方法で算出された閾値は、少なくとも１回のパスワード認証動作（１つ認証結果が得られるまでの動作期間）中は固定して使用するものとする。

【００３１】その他に、はじめに適当な初期値を閾値として与えておき、以後、実際に測定された単位時間当たりのパスワード受信回数に基づいて動的に閾値を変更して行く方法がある。

【００３２】例えば、図５に示すように、単位時間当たりのパスワード受信回数の計測値と閾値との比較で、閾値未満の計測値つまり人間の手入力によるものとみなせる計測値を記憶し、この計測値がｎ個（ｎは１以上の整数）得られる度に、これら計測値を用いて閾値を計算し直す方法が考えられる。この場合、①の方法により、ｎ個の計測値の平均値を求め、平均値＋標準偏差×ｎを新たな閾値とする。

【００３３】また、図６に示すように、計測値と閾値との比較で、閾値以上の計測値つまり機械的パスワード推測によるものとみなせる計測値を記憶し、この計測値がｎ個（ｎは１以上の整数）得られる度に、これら計測値を用いて閾値を計算し直す方法も考えられる。この場合、②の方法により、ｎ個の計測値の平均値を求め、平均値＋標準偏差×ｎを新たな閾値とする。

【００３４】次に、受信パスワードに関する情報として“パスワードの入力時間間隔”を用いた場合のパスワード認証方法の実施形態２について説明する。“パスワードの入力時間間隔”の場合、具体的にはその“平均値”や“入力時間間隔のばらつきの大きさ”が測定対象となる。

【００３５】（実施形態２－１）まず“パスワードの入

力時間間隔の平均値”を用いた場合について説明する。図７はこの場合のパスワード認証手順を示すフローチャートである。パスワード受信部１１はパスワードＰｉを受信する度に、パスワード受信時刻Ｔｉを記憶すると共に１つ前に受信したパスワードの受信時刻Ｔi-1との時間間隔Ｄｉを測定して記憶する（ステップ７０１～７０６）。パスワード受信部１１は、ｎ（ｎ≧２）回パスワードを受信したところで（ステップ７０７）、記憶されたｎ－１個のパスワード入力時間間隔の平均値ａを求め（ステップ７０８）、この平均値ａを閾値比較部１４に送る。

【００３６】閾値比較部１４は、パスワードの入力時間間隔の平均値ａと閾値計算部１３にて予め設定された閾値Ｇとを比較する（ステップ７０９）。ここで閾値Ｇは、プログラム等による機械的パスワード推測時のパスワード入力時間間隔が手入力時のパスワード入力時間間隔より短いという仮説に基づいて最適に設定される。その具体的な設定方法は“単位時間当たりのパスワード受信回数”の閾値設定方法と同様の方法を用いることができる。

【００３７】上記比較の結果、ａ≦Ｇの場合は、機械的パスワード推測が行われているとみなし、認証失敗を判定する。また、ａ＞Ｇの場合は、受信したｎ個のパスワードをパスワード認証部１２に送る。パスワード認証部１２は受信パスワードの中に正しいパスワードがあれば認証成功を判断し、システム資源のアクセス権限をクライアント計算機１上の利用者に与える。また、受信パスワードの中に正しいパスワードがなければ再びパスワード受信を行う（ステップ７１０～７１３）。

【００３８】このようにパスワードの認証を行う前に、パスワードの入力時間間隔の平均値ａと閾値Ｇとを比較して機械的パスワード推測が行われているかどうかを判断することで、機械的パスワード推測によって偶然正しいパスワードが入力されても認証失敗としてシステム資源のアクセス権限を誤って不正な利用者に与えることを防止できる。

【００３９】（実施形態２－２）次に、受信パスワードに関する情報として“パスワードの入力時間間隔の平均値”を用いた場合のもう一つのパスワード認証方法について説明する。

【００４０】図８はこの場合のパスワード認証方法の手順を示すフローチャートである。パスワード受信部１１はパスワードＰｉを受信する度に、パスワード受信時刻Ｔiを記憶すると共に、その受信パスワードをパスワード認証部１２に送ってパスワード認証を実施させる。受信パスワードが正しいパスワードがあれば認証成功を判断し、システム資源のアクセス権限をクライアント計算機１上の利用者に与える。また、受信パスワードが誤ったパスワードでなければ１つ前に受信したパスワードの受信時刻Ｔi-1との時間間隔Ｄｉを測定して記憶する（ステップ８０１～８０９）。パスワード受信部１１は、ｎ（ｎ≧２）回連続して誤ったパスワードが入力された場合、記憶されたｎ－１個のパスワードの入力時間間隔の平均値ａを求め（ステップ８１０、８１１）、この平均値ａを閾値比較部１４に送る。閾値比較部１４は、パスワードの入力時間間隔の平均値ａと閾値計算部１３にて予め設定された閾値Ｇとを比較する（ステップ８１２）。上記比較の結果、ａ≦Ｇａの場合は、機械的パスワード推測が行われているとみなし、認証失敗を判定する。また、ａ＞Ｇの場合は次のパスワード受信を行う。

【００４１】このパスワード認証方法によれば、最初のｎ回のパスワード受信を除けば、機械的パスワード推測によって偶然正しいパスワードが入力されても認証失敗を判定することができる。なお、最初のｎ回以内に機械的パスワード推測によって偶然正しいパスワードが入力される確率は極めて低く実用上全く問題はない。また、このパスワード認証方法は、前記の方法と比較した場合、ｎ回のパスワード受信による遅延を有することなくパスワードの認証結果を利用者に提供することができ、利用者に違和感を与えない方法と言える。

【００４２】（実施形態２－３）ところで、上記実施形態２－１、２－２のパスワード認証方法は、プログラム等による機械的パスワード推測時のパスワード入力時間間隔が手入力時のパスワード入力時間間隔より短いという仮説に基づくものであるが、機械的パスワード推測時のパスワードの入力時間間隔のばらつきは手入力時のパスワード入力時間間隔のばらつきよりも小さいという仮説に基づいて同様のパスワード認証を行うことが可能である。

【００４３】この場合、図９及び図１０に示すように、そのステップ９０８及びステップ１０１１にて、記憶されたｎ－１個のパスワードの入力時間間隔Ｄi の分散（あるいは標準偏差）をパスワード入力時間間隔のばらつきの大きさａとして求め、このパスワード入力時間間隔のばらつきの大きさａと閾値Ｇとを比較し、ａ≦Ｇの場合、機械的パスワード推測が行われているとみなし、認証失敗を判定する。なお、図９及び図１０図のその他のステップの内容は図７及び図８と同じである。かくして、この“パスワード入力時間間隔のばらつきの大きさ”を用いたパスワード認証方法によっても、機械的パスワード推測を高精度に検出でき、システム資源のアクセス権限を不正な利用者に与えることを防止できる。

【００４４】次に、受信パスワードに関する情報として“パスワード間の類似度”を用いた場合のパスワード認証方法の実施形態３について説明する。

【００４５】本実施形態において、パスワード受信部１１はパスワードを受信する度にこのパスワードを記憶すると共に、このパスワードと１つ前に受信したパスワードとを比較し、その比較結果である入力パスワード間の

類似度ａを閾値比較部１４に送る。閾値比較部１４は、入力パスワード間の類似度ａと閾値計算部１３にて予め設定された閾値Ｇとを比較し、これらの大小関係を基に機械的パスワード推測を検出する。

【００４６】ここで“パスワード間の類似度”は“パスワード間の共通する位置の文字が一致しているものの数”“辞書編纂順に並んだパスワードの数”“文字列が完全に一致する２つのパスワードの組み合わせの数”等により定義される。

【００４７】（実施形態３－１）“パスワード間の共通する位置の文字が一致しているものの数”とは、具体的には、連続する２つのパスワードにおいて先頭からｊ番目（ｊは２つのパスワードにおいて文字数が少ない方の文字数以下の所定数）までの各文字列の同じ位置の文字が一致しているものの数を言う。例えば“あいうえお…”“あいかきお”の２つのパスワード間の同一文字数は“あ”“い”“お”の３である。このように、連続する２つのパスワード間の共通する位置の文字が一致しているものの数をｎ（ｎは２以上の所定数）個の連続するパスワードについて求め、その平均値を２つのパスワードにおいて文字数が少ない方の文字数で割った値をパスワード間の類似度ａとして閾値Ｇと比較する。そしてａ≧Ｇの場合に機械的パスワード推測が行われているとみなし、認証失敗を判定する。すなわち、このパスワード認証は、機械的パスワード推測が少しずつ（例えば１文字ずつ）パスワードを変えながら行われることが多いと言う仮説に基づくものである。

【００４８】（実施形態３－２）“辞書編纂順に並んだパスワードの数”とは、具体的には、連続して入力されたｎ個のパスワード単語のうち連続して辞書編纂順（昇順或いは降順）となっているパスワード単語の数を言う。この連続して辞書編纂順となっているパスワードの数をパスワード間の類似度ａとして閾値Ｇと比較し、ａ≧Ｇの場合を機械的パスワード推測が行われているとみなし、認証失敗を判定する。

【００４９】パスワードとして単語が使用される確率は非常に高いことから、機械的パスワード推測においては辞書の単語を編纂順に入力することが考えられる。このような機械的パスワード推測を本実施形態のパスワード認証方法は極めて高精度に検出することが可能である。

【００５０】（実施形態３－３）さらに“パスワード間の類似度”を用いたその他のパスワード認証方法について述べる。ｎ個のパスワード間において文字列が完全に一致する２つのパスワードの組み合わせの数を求め、全てのパスワードの組み合わせの数に対する一致パスワードの組み合わせの数の割合をパスワード間の類似度ａとして求める。そしてこの類似度ａと閾値Ｇと比較し、ａ＜Ｇの場合を機械的パスワード推測が行われているとみなし、認証失敗を判定する。この方法は、人間によるパスワード入力においては同じパスワードがしばしば入力されるが、機械的パスワード推測によるパスワード入力であれば同じパスワードを入力することはまず無いという仮説に基づくものである。

【００５１】以上の実施形態３－１～３－３のパスワード認証方法においても“パスワード間の類似度”の計算結果ａと閾値Ｇとの比較による機械的パスワード推測の検出を行ってからパスワードの認証を行う方法と、パスワードを受信する度にパスワードの認証を行う方法が考えられる。

【００５２】なお、以上説明した各実施形態のパスワード認証方法は、複数組み合わせて採用することが精度向上を図るうえにおいて効果的である。

【００５３】

【発明の効果】以上説明したように本発明のパスワード認証方法によれば、正規利用者にとってのパスワードの使い勝手を悪くすることなく、機械的パスワード推測を高精度に検出することができ、システム資源のアクセス権限を不正な利用者に与えることを防止できる。

【図面の簡単な説明】

【図１】本発明に係るパスワード認証方法を採用したコンピュータシステムの構成を示す図

【図２】図１のサーバ計算機内のパスワード認証機構の構成を示すブロック図

【図３】本発明の実施形態１－１のパスワード認証方法の手順を示すフローチャート

【図４】本発明の実施形態１－２のパスワード認証方法の手順を示すフローチャート

【図５】本発明に係るパスワード認証方法に用いられる閾値の動的な設定方法を示すフローチャート

【図６】同じく閾値の動的な設定方法を示すフローチャート

【図７】本発明の実施形態２－１のパスワード認証方法の手順を示すフローチャート

【図８】本発明の実施形態２－２のパスワード認証方法の手順を示すフローチャート

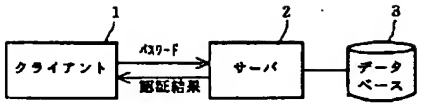
【図９】本発明の実施形態２－３のパスワード認証方法の手順を示すフローチャート

【図１０】本発明の実施形態２－３のもう一つのパスワード認証方法の手順を示すフローチャート

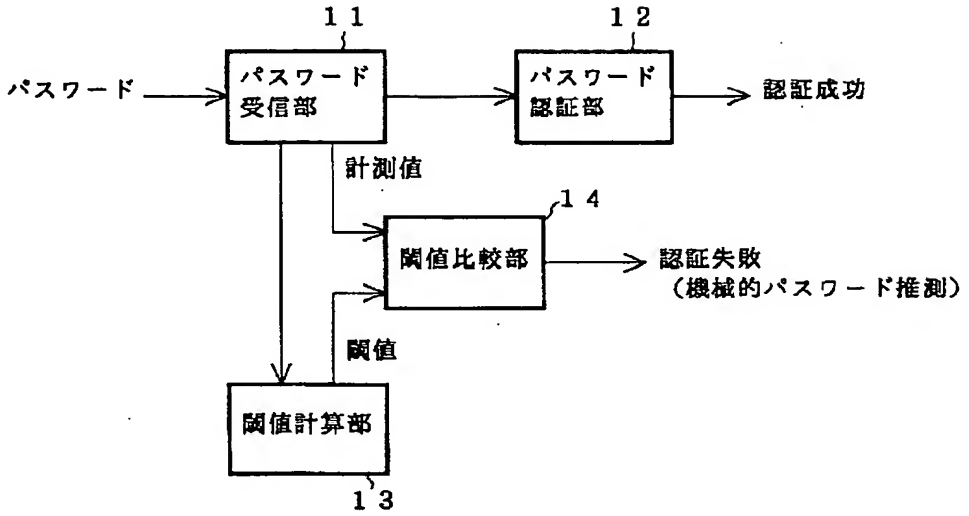
【符号の説明】

１……クライアント計算機
２……サーバ計算機
３……データベース（システム資源）
１１……パスワード受信部
１２……パスワード認証部
１３……閾値計算部
１４……閾値比較部

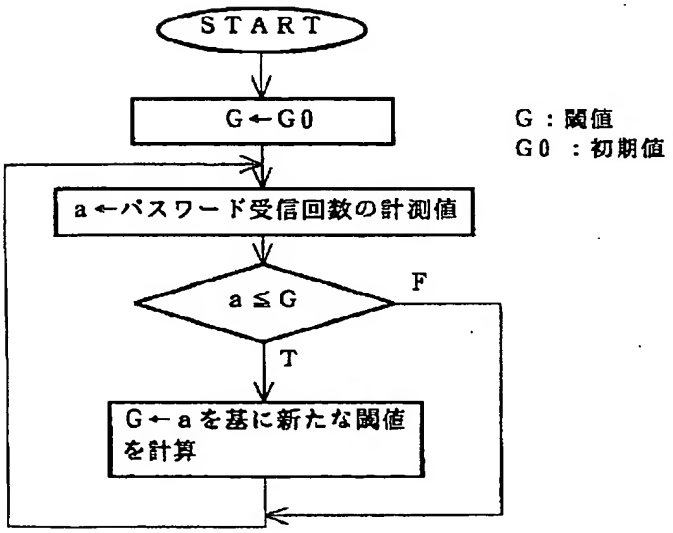
【図１】



【図２】

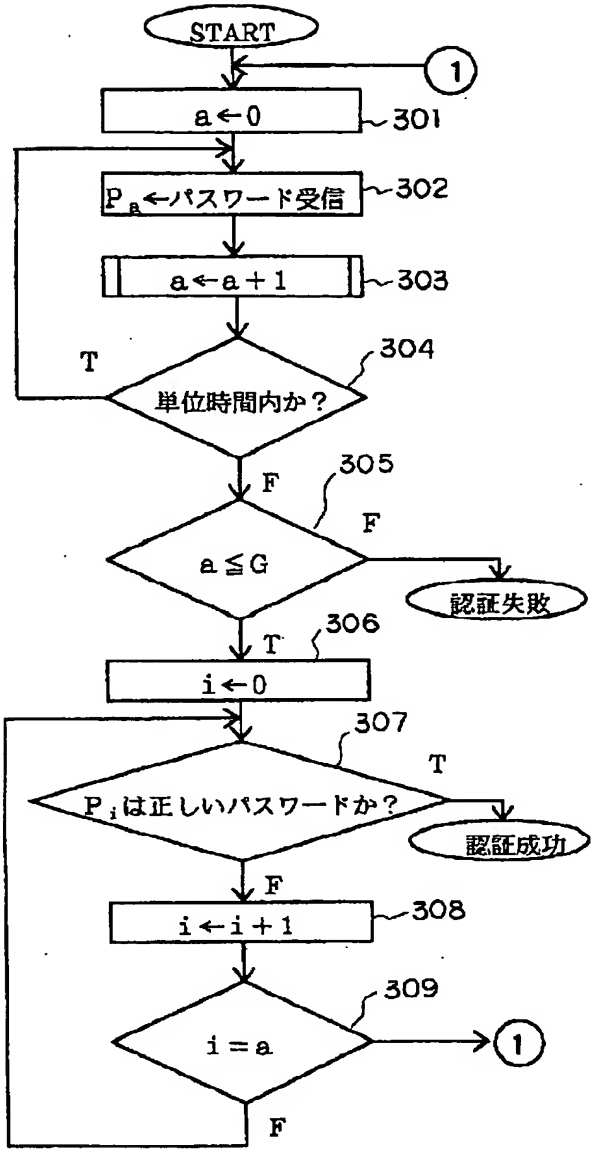


【図５】

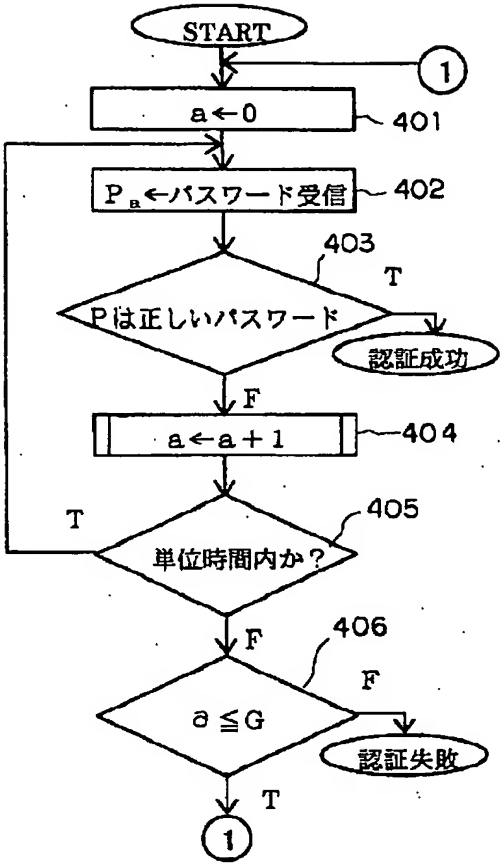


G：閾値
G0：初期値

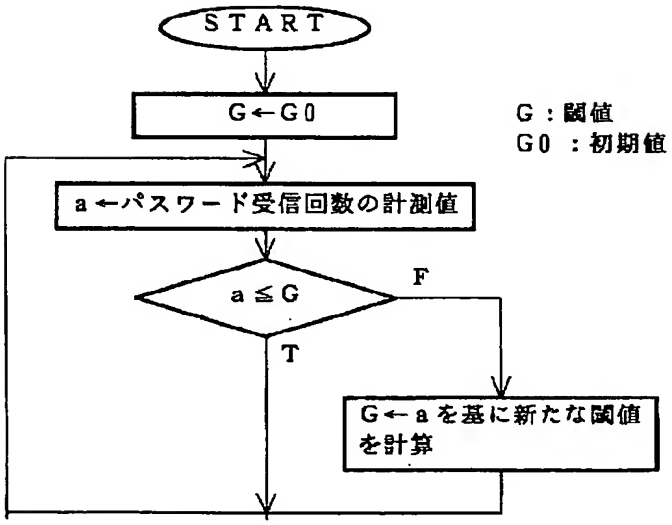
【図３】


START
1
a←0
301
P_a←パスワード受信
302
a←a＋1
303
T
304
単位時間内か？
F
305
F
a≦G
認証失敗
T
306
i←0
307
T
P_iは正しいパスワードか？
認証成功
F
i←i＋1
308
309
i＝a
1
F

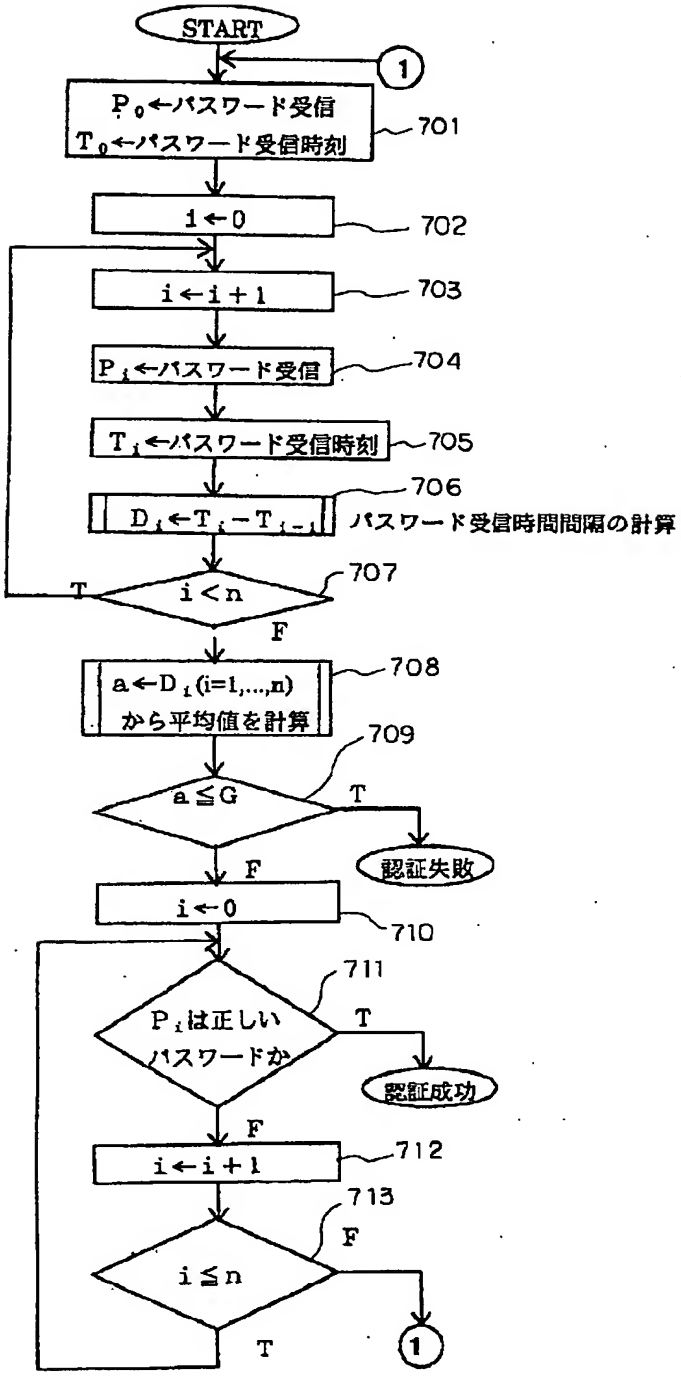
【図４】


START
1
a←0
401
Pa←パスワード受信
402
403
T
Pは正しいパスワード
認証成功
F
a←a＋1
404
T
405
単位時間内か？
F
406
F
a≦G
認証失敗
T
1

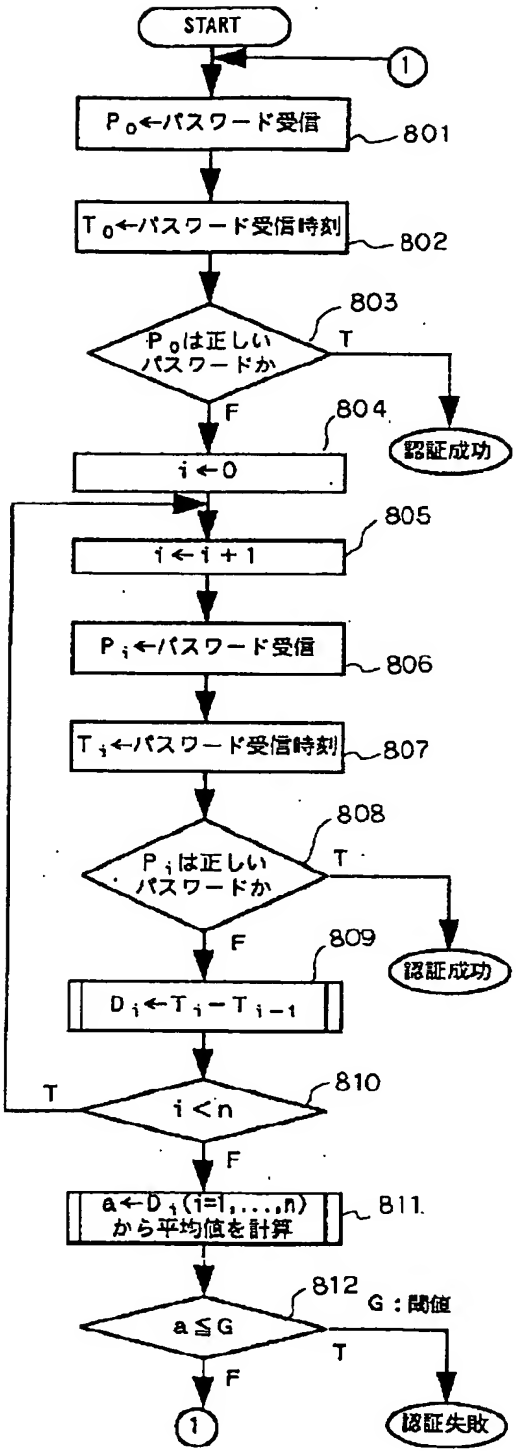
【図６】


START
G←G0
G：閾値
G0：初期値
a←パスワード受信回数の計測値
a≦G
F
T
G←aを基に新たな閾値を計算

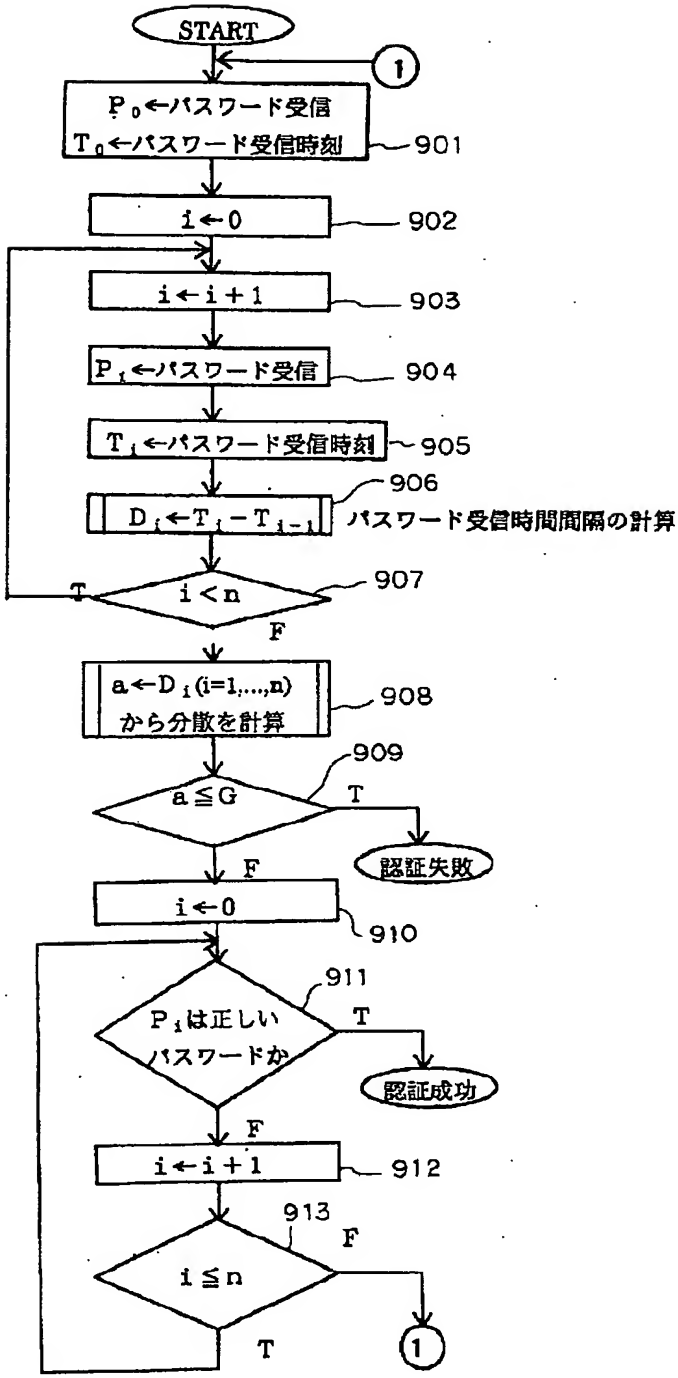
【図７】


START
1
P0←パスワード受信
T0←パスワード受信時刻
701
i←0
702
i←i+1
703
Pi←パスワード受信
704
Ti←パスワード受信時刻
705
706
Di←Ti−Ti−1
パスワード受信時間間隔の計算
i<n
707
T
F
a←Di(i=1,...,n)
から平均値を計算
708
709
a≦G
T
認証失敗
F
i←0
710
711
Piは正しい
パスワードか
T
認証成功
F
i←i+1
712
713
F
i≦n
T
1

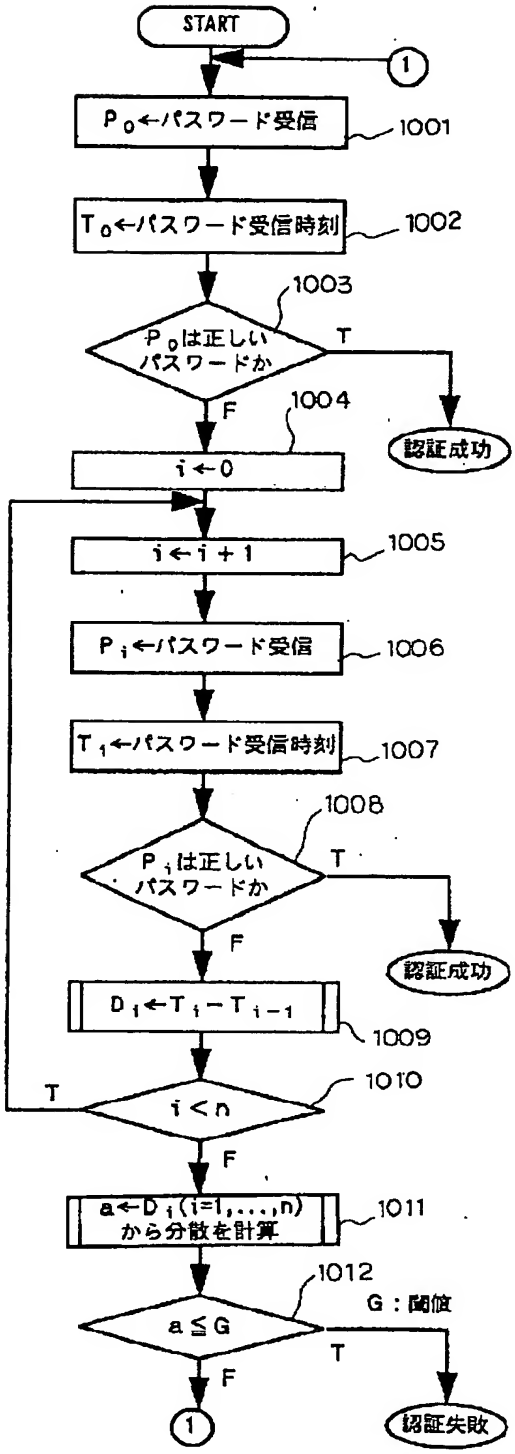
【図８】


START
1
P₀←パスワード受信
801
T₀←パスワード受信時刻
802
803
P₀は正しいパスワードか
T
F
804
認証成功
i←0
805
i←i+1
Pᵢ←パスワード受信
806
Tᵢ←パスワード受信時刻
807
808
Pᵢは正しいパスワードか
T
F
809
認証成功
Dᵢ←Tᵢ−Tᵢ₋₁
T
i<n
810
F
a←Dᵢ(i=1,...,n)から平均値を計算
811
812
G：閾値
a≦G
T
F
1
認証失敗

【図９】


START
1
P_0←パスワード受信
T_0←パスワード受信時刻
901
i←0
902
i←i＋1
903
P_i←パスワード受信
904
T_i←パスワード受信時刻
905
906
D_i←T_i－T_{i-1}
パスワード受信時間間隔の計算
T
i＜n
907
F
a←D_i(i=1,...,n)
から分散を計算
908
909
a≦G
T
認証失敗
F
i←0
910
911
P_iは正しい
パスワードか
T
認証成功
F
i←i＋1
912
913
F
i≦n
T
1

【図１０】


START
1
P0←パスワード受信
1001
T0←パスワード受信時刻
1002
1003
P0は正しいパスワードか
T
F
認証成功
1004
i←0
i←i+1
1005
Pi←パスワード受信
1006
Ti←パスワード受信時刻
1007
1008
Piは正しいパスワードか
T
F
認証成功
Di←Ti−Ti−1
1009
T
i<n
1010
F
a←Di(i=1,...,n)から分散を計算
1011
1012
G：閾値
a≦G
T
F
1
認証失敗